Ref-2

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2004-038445

(43)Date of publication of application : 05.02.2004

(51)Int.CI. G06K 19/10
B42D 15/10
G06K 17/00
G06K 19/073
H04L 9/08
H04L 9/10
H04L 9/32

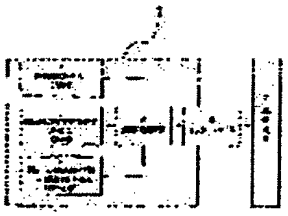
(21)Application number : 2002-193162

(22)Date of filing : 02.07.2002

(71)Applicant : NEC TOKIN CORP

(72)Inventor : ARAI ATSUSHI

(54) IC CARD AND ENCRYPTION METHOD FOR THE SAME



(57)Abstract:

PROBLEM TO BE SOLVED: To obtain an IC card for transmitting a telegram with high confidentiality and integrity by performing secure messaging using a key of a public key encryption system.

SOLUTION: In an IC car and a higher-order device with a read only nonvolatile memory and a readable/writable nonvolatile memory, when the IC card transfers the telegram to the higher-order device, the IC card recognizes the confidentiality and integrity of the telegram by using two sets of paired public keys and secret keys.

Ref-2

対応なし、英抄

(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-38445
(P2004-38445A)
(43)公開日　平成16年2月5日(2004.2.5)

(51)Int.Cl.[7]		F I			テーマコード（参考）
G06K	19/10	G06K	19/00	R	2C005
B42D	15/10	B42D	15/10	521	5B035
G06K	17/00	G06K	17/00	S	5B058
G06K	19/073	G06K	19/00	P	5J104
H04L	9/08	H04L	9/00	621A	

審査請求 有　請求項の数 14　ＯＬ　（全 9 頁）　最終頁に続く

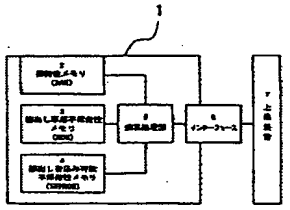
(21)出願番号　特願2002-193162(P2002-193162)
(22)出願日　平成14年7月2日(2002.7.2)

(71)出願人　000134257
ＮＥＣトーキン株式会社
宮城県仙台市太白区郡山６丁目７番１号
(72)発明者　荒井　篤志
宮城県仙台市太白区郡山六丁目７番１号
エヌイーシートーキン株式会社内

Ｆターム(参考)　2C005 MA01 SA02 SA23
5B035 AA13 BB09 CA38
5B058 CA01 KA31 KA35
5J104 AA16 EA04 EA15 NA02 NA12
NA35

(54)【発明の名称】ＩＣカードおよびＩＣカードの暗号方法

(57)【要約】
【課題】公開鍵暗号方式の鍵を使用したセキュアメッセージングを行うことにより、隠蔽性、完全性の高い電文を送信することができるＩＣカードを得る。
【解決手段】少なくとも演算処理部、揮発性メモリ、読み出し専用不揮発性メモリ及び読み出し書き込み可能な不揮発性メモリを具備したＩＣカード及び上位装置において、上位装置との電文の伝送において、対となっている公開鍵及び秘密鍵を２組使用して、前記電文の隠蔽及び完全性の確認を行うＩＣカードとする。
【選択図】　図１



【特許請求の範囲】
【請求項１】
少なくとも演算処理部、揮発性メモリ、読み出し専用不揮発性メモリ及び読み出し書き込み可能な不揮発性メモリを具備したＩＣカード及び上位装置において、上位装置との電文の伝送において、対となっている公開鍵及び秘密鍵を２組使用して、前記電文の隠蔽及び完全性の確認を行うことを特徴とするＩＣカード。
【請求項２】
前記ＩＣカードが保持している公開鍵対の公開鍵を上位装置が持ち、前記上位装置が保持している公開鍵対の公開鍵を前記ＩＣカードが持ち、前記２つの公開鍵対を伝送する電文の隠蔽及び完全性の確認に使用することを特徴とする請求項１に記載のＩＣカード。
【請求項３】
前記ＩＣカードが起動後に前記ＩＣカードの持つ公開鍵対の公開鍵を上位装置に渡し、前記上位装置が起動後に前記上位装置の持つ公開鍵対の公開鍵を前記ＩＣカードに渡し、前記２つの公開鍵対を伝送する電文の隠蔽及び完全性の確認に使用することを特徴とする請求項１または２に記載のＩＣカード。
【請求項４】
前記上位装置へ隠蔽及び完全性確認を行った電文をＩＣカードが送信する際に、前記上位装置が持つ公開鍵対の公開鍵を用いて平文を暗号化することで隠蔽を行い、前記ＩＣカードが持つ公開鍵対の秘密鍵を用いて、完全性確認のための認証子の暗号化を行うことで完全性の確認を行うことを特徴とする請求項１ないし３のいずれかに記載のＩＣカード。
【請求項５】
前記上位装置から隠蔽及び完全性確認を行った電文をＩＣカードが受信した際に、前記上位装置が持つ公開鍵対の公開鍵を用いて、完全性確認のための認証子の復号化を行うことで完全性の確認を行い、前記ＩＣカードが持つ公開鍵対の秘密鍵を用いて、隠蔽された暗号文を復号化することを特徴とする請求項１ないし３のいずれかに記載のＩＣカード。
【請求項６】
前記ＩＣカードの動作終了時に前記ＩＣカードが上位装置から受け取り、電文の隠蔽且つ完全性確認に使用した公開鍵を廃棄することを特徴とする請求項１ないし５のいずれかに記載のＩＣカード。
【請求項７】
前記ＩＣカード起動後に前記ＩＣカードが、前記ＩＣカード内で作製した乱数により上位装置に渡す公開鍵を含む公開鍵対を新たに作製することを特徴をする請求項１ないし５のいずれかに記載のＩＣカード。
【請求項８】
前記ＩＣカードが持つ電文の隠蔽且つ完全性の確認に使用する公開鍵対が読み出し専用不揮発性メモリに格納されていることを特徴とする請求項１ないし５のいずれかに記載のＩＣカード。
【請求項９】
前記ＩＣカード起動後に交換される上位装置の公開鍵が揮発性メモリに格納されることを特徴とする請求項１ないし８のいずれかに記載のＩＣカード。
【請求項１０】
前記ＩＣカード起動後に交換される上位装置の公開鍵が、読み出し書き込み可能な不揮発性メモリに格納されることを特徴とする請求項１ないし８のいずれかに記載のＩＣカード。
【請求項１１】
前記ＩＣカード起動後に交換される上位装置の公開鍵を前記ＩＣカードの動作終了時まで使用することを特徴とする請求項９または１０に記載のＩＣカード。
【請求項１２】
少なくとも演算処理部、揮発性メモリ、読み出し専用不揮発性メモリ及び読み出し書き込み可能な不揮発性メモリを具備したＩＣカードの認証方法において、ＩＣカードと上位装

置との電文の伝送において、対となっている公開鍵及び秘密鍵を２組使用して、前記電文の隠蔽及び完全性の確認を行うことを特徴とするＩＣカードの暗号方法。
【請求項１３】
前記ＩＣカードの暗号方法は、ＩＣカードがセキュア電文を送信し、上位装置がセキュア電文を受信する場合に、上位装置は対となる第１の秘密鍵１０と第１の公開鍵１１を有し、前記ＩＣカードは、前記上位装置より前記第１の公開鍵を取得し、前記ＩＣカードは、取得した第１の公開鍵を、ＩＣカード内のＲＡＭまたはＥＥＰＲＯＭに格納し、前記ＩＣカードは、そのカード内部に、対となる第２の秘密鍵、第２の公開鍵を生成し、ついで、前記ＩＣカードは第２の公開鍵を前記上位装置へ送信し、前記ＩＣカードは、第１の公開鍵を使用して、上位装置に送信する平文を暗号化し暗号文を作成し、前記ＩＣカードは、前記暗号文よりハッシュ値を作成し、前記ＩＣカードは、前記ハッシュ値と第２の秘密鍵よりメッセージ認証子を作成し、前記ＩＣカードは、メッセージ認証子を添付した暗号文を、上位装置に対して送信し、前記メッセージ認証子を添付した暗号文を受信した上位装置は、暗号文からハッシュ値を作成し、前記上位装置は、メッセージ認証子を第２の公開鍵を用いて復号化し、前記上位装置は、復号化したハッシュ値と、作成したハッシュ値を比較し、前記上位装置は、暗号文を第１の秘密鍵を使用して復号化し、ＩＣカードより送信された平文を取り出すことを特徴とする請求項１２に記載のＩＣカードの暗号方法。
【請求項１４】
前記ＩＣカードの暗号方法は、上位装置がセキュア電文を送信し、ＩＣカードがセキュア電文を受信する場合に、上位装置は対となる第１の秘密鍵１０と第１の公開鍵１１を有し、前記ＩＣカードは、前記上位装置より前記第１の公開鍵を取得し、前記ＩＣカードは、取得した第１の公開鍵を、ＩＣカード内のＲＡＭまたはＥＥＰＲＯＭに格納し、前記ＩＣカードは、そのカード内部に、対となる第２の秘密鍵、第２の公開鍵を生成し、ついで、前記ＩＣカードは第２の公開鍵を前記上位装置へ送信し、上位装置は、第２の公開鍵を使用してＩＣカードに送信する平文を暗号化し、暗号文を作成し、前記上位装置は、前記暗号文よりハッシュ値を作成し、前記上位装置は、前記ハッシュ値と第１の秘密鍵より、メッセージ認証子を作成し、上位装置は、前記メッセージ認証子を添付した暗号文をＩＣカードに対して送信し、前記メッセージ認証子を添付した暗号文を受信した、ＩＣカードは、暗号文からハッシュ値を作成し、前記ＩＣカードは、前記メッセージ認証子を第１の公開鍵を用いて復号化し、ＩＣカードは、前記復号化したハッシュ値と、作成したハッシュ値を比較し、ＩＣカードは、暗号文を第２の秘密鍵を使用して復号化し、ＩＣカードより送信された平文を取り出すことを特徴とする請求項１２に記載のＩＣカードの暗号方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、主としてＩＣカード及びその周辺装置との通信に際し、より秘密性の高い隠蔽及び完全性の確認を行うのに好適なＩＣカードおよびＩＣカードの暗号方法に関する。
【０００２】
【従来の技術】
ＩＣカードの通信と上位装置で通信する電文の隠蔽及び完全性確認（以後、セキュアメッセージングという）を行う場合には、一般的には共通鍵暗号方式の鍵が使用されていた。
【０００３】
【発明が解決しようとする課題】
しかし、従来の共通鍵暗号方式では、ＩＣカード側と、上位装置側とで共通鍵を使用していたために、以下の問題点があった。即ち、共通鍵を使用しているので、第三者が故意に共通鍵を盗んで使用すれば、暗号は解読されてしまう。従って、従来の共通鍵圧電方式は、秘密保持の点でセキュリティが不十分であり、隠蔽性が劣るものであった。
【０００４】
従って、本発明の目的は、公開鍵暗号方式の鍵を使用したセキュアメッセージングを行うことにより、隠蔽性、完全性の高い電文を送信することができるＩＣカードおよびＩＣカ

ードの暗号方法を提供することである。
【０００５】
【課題を解決するための手段】
本発明のＩＣカードは、少なくとも演算処理部、揮発性メモリ、読み出し専用不揮発性メモリ及び読み出し書き込み可能な不揮発性メモリを具備したＩＣカード及び上位装置において、上位装置との電文の伝送において、以後、公開鍵対を２組使用して、前記電文の隠蔽及び完全性の確認を行う機能を有するＩＣカードである。
【０００６】
更に、本発明のＩＣカードは、ＩＣカードが保持している公開鍵対の公開鍵を上位装置が持ち、前記上位装置が保持している公開鍵対の公開鍵を前記ＩＣカードが持ち、前記２つの公開鍵対を伝送する電文の隠蔽及び完全性の確認に使用する機能を有するＩＣカードである。
【０００７】
また、使用する公開鍵対を前記ＩＣカードが起動後にＩＣカードの持つ公開鍵対の公開鍵を上位装置に渡し、前記上位装置が起動後に上位装置の持つ公開鍵対の公開鍵をＩＣカードに渡し、前記２つの公開鍵対を伝送する電文の隠蔽及び完全性の確認に使用する機能を有するＩＣカードである。
【０００８】
更に、本発明のＩＣカードは、上位装置へ隠蔽及び完全性確認を行った電文を送信する際に、前記上位装置が持つ公開鍵対の公開鍵を用いて平文を暗号化することで隠蔽を行い、前記ＩＣカードが持つ公開鍵対の秘密鍵を用いて、完全性確認のための認証子の暗号化を行うことで完全性の確認を行う機能を有するＩＣカードである。
【０００９】
続いて、上位装置から隠蔽及び完全性確認を行った電文を受信した際に、前記上位装置が持つ公開鍵対の公開鍵を用いて、完全性確認のための認証子の復号化を行うことで完全性の確認を行い、前記ＩＣカードが持つ公開鍵対の秘密鍵を用いて、隠蔽された暗号文を復号化することを行う機能を有するＩＣカードである。
【００１０】
更に、本発明のＩＣカードは、上位装置から受け取った公開鍵をＩＣカードの動作終了時に使用した前記公開鍵が廃棄される機能を有するＩＣカードである。
【００１１】
更に、上位装置に渡す公開鍵を含む公開鍵対をＩＣカード起動後にＩＣカード内で作成した乱数により新たに作成する機能を有するＩＣカードである。
【００１２】
更に、本発明のＩＣカードは、電文の隠蔽且つ完全性の確認に使用する前記ＩＣカードが持つ公開鍵対が読み出し専用不揮発性メモリに格納する機能を有するＩＣカードである。
【００１３】
または、ＩＣカード起動後に交換される前記上位装置の公開鍵が揮発性メモリに格納される機能を有するＩＣカードである。
【００１４】
または、ＩＣカード起動後に交換される前記上位装置の公開鍵が読み出し書き込み可能な不揮発性メモリに格納される機能を有するＩＣカードである。
【００１５】
また、本発明は、少なくとも演算処理部、揮発性メモリ、読み出し専用不揮発性メモリ及び読み出し書き込み可能な不揮発性メモリを具備したＩＣカードの認証方法において、ＩＣカードと上位装置との電文の伝送において、対となっている公開鍵及び秘密鍵を２組使用して、前記電文の隠蔽及び完全性の確認を行うＩＣカードの暗号方法である。
【００１６】
また、本発明は、前記ＩＣカードの暗号方法は、ＩＣカードがセキュア電文を送信し、上位装置がセキュア電文を受信する場合に、上位装置は対となる第１の秘密鍵１０と第１の

公開鍵１１を有し、前記ＩＣカードは、前記上位装置より前記第１の公開鍵を取得し、前記ＩＣカードは、取得した第１の公開鍵を、ＩＣカード内のＲＡＭまたはＥＥＰＲＯＭに格納し、前記ＩＣカードは、そのカード内部に、対となる第２の秘密鍵、第２の公開鍵を生成し、ついで、前記ＩＣカードは第２の公開鍵を前記上位装置へ送信し、前記ＩＣカードは、第１の公開鍵を使用して、上位装置に送信する平文を暗号化し暗号文を作成し、前記ＩＣカードは、前記暗号文よりハッシュ値を作成し、前記ＩＣカードは、前記ハッシュ値と第２の秘密鍵よりメッセージ認証子を作成し、前記ＩＣカードは、メッセージ認証子を添付した暗号文を、上位装置に対して送信し、前記メッセージ認証子を添付した暗号文を受信した上位装置は、暗号文からハッシュ値を作成し、前記上位装置は、メッセージ認証子を第２の公開鍵を用いて復号化し、前記上位装置は、復号化したハッシュ値と、作成したハッシュ値を比較し、前記上位装置は、暗号文を第１の秘密鍵を使用して復号化し、ＩＣカードより送信された平文を取り出すＩＣカードの暗号方法である。

【００１７】

また、本発明は、上位装置がセキュア電文を送信し、ＩＣカードがセキュア電文を受信する場合に、前記ＩＣカードの暗号方法は、上位装置は対となる第１の秘密鍵１０と第１の公開鍵１１を有し、前記ＩＣカードは、前記上位装置より前記第１の公開鍵を取得し、前記ＩＣカードは、取得した第１の公開鍵を、ＩＣカード内のＲＡＭまたはＥＥＰＲＯＭに格納し、前記ＩＣカードは、そのカード内部に、対となる第２の秘密鍵、第２の公開鍵を生成し、ついで、前記ＩＣカードは第２の公開鍵を前記上位装置へ送信し、上位装置は、第２の公開鍵を使用してＩＣカードに送信する平文を暗号化し、暗号文を作成し、前記上位装置は、前記暗号文よりハッシュ値を作成し、前記上位装置は、前記ハッシュ値と第１の秘密鍵より、メッセージ認証子を作成し、上位装置は、前記メッセージ認証子を添付した暗号文をＩＣカードに対して送信し、前記メッセージ認証子を添付した暗号文を受信した、ＩＣカードは、暗号文からハッシュ値を作成し、前記ＩＣカードは、前記メッセージ認証子を第１の公開鍵を用いて復号化し、ＩＣカードは、前記復号化したハッシュ値と、作成したハッシュ値を比較し、ＩＣカードは、暗号文を第２の秘密鍵を使用して復号化し、ＩＣカードより送信された平文を取り出すＩＣカードの暗号方法である。

【００１８】

【発明の実施の形態】

以下、本発明の実施の形態によるＩＣカードおよびＩＣカードの暗号方法について、ＩＣカード本体およびＩＣカードがセキュアメッセージシグ処理された電文（以後、セキュア電文という）を送信する場合とＩＣカードがセキュア電文を受信する場合とに分けて図面を用いて詳細に説明する。

【００１９】

（実施の形態１）

図１は、本発明の実施の形態１によるＩＣカードの構成例を示したものである。本実施の形態のＩＣカード１内に搭載されたＩＣチップ上には、上位装置７とデータ交換を行うインタフェース６と制御プログラムを処理する演算処理部５と、揮発性メモリ（ＲＡＭ）２と、制御プログラムを格納しておく読み出し専用不揮発性メモリ（ＲＯＭ）３と、書き込みまたは書き換えデータを格納する読み出し書き込み可能不揮発性メモリ（ＥＥＰＲＯＭ）４が具備されている。

【００２０】

（実施の形態２）

図２は、本発明の実施の形態２によるＩＣカードの暗号方法の模式図であり、ＩＣカード９がセキュア電文を送信し、上位装置８がセキュア電文を受信する場合の模式図である。

（１）上位装置８は対となる秘密鍵１０と公開鍵１１を持っている。

（２）ＩＣカード９は上位装置８より公開鍵１１を取得する。

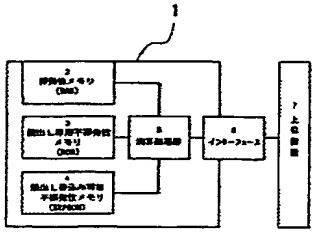
（３）ＩＣカード９は、取得した公開鍵１１を揮発性メモリ２または読み出し書き込み可能不揮発性メモリ４に格納する。

（４）ＩＣカード９は、そのカード内部に対となる秘密鍵１２、公開鍵１３を生成する又

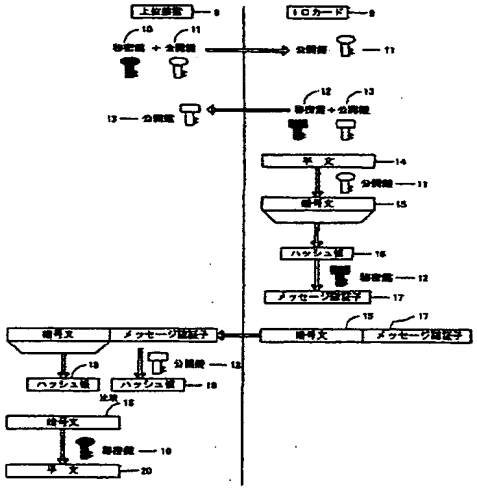
は持っている。
（５）ＩＣカード９は公開鍵１３を上位装置へ送信する。
（６）ＩＣカード９は公開鍵１１を使用して上位装置に送信する平文１４を暗号化し暗号文１５を作成する。
（７）ＩＣカード９は暗号文１５よりハッシュ値１６を作成する。
（８）ＩＣカード９はハシシュ値１６と秘密鍵１２よりメッセージ認証子１７を作成する。
（９）ＩＣカード９はメッセージ認証子１７を添付した暗号文１５を上位装置８に対して送信する。
（１０）メッセージ認証子１７を添付した暗号文１５を受信した上位装置８は暗号文１６からハッシュ値１８を作成する。
（１１）上位装置８はメッセージ認証子１７を公開鍵１３を用いて復号化する。
（１２）上位装置８は復号化したハッシュ値１９と作成したハッシュ値１８を比較する。
（１３）上位装置８は暗号文１５を秘密鍵１０を使用して復号化し、ＩＣカードより送信された平文２０を取りだす。
【００２１】
（実施の形態３）
図３は、本発明の実施の形態３によるＩＣカードの暗号方法の模式図であり、上位装置８がセキュア電文を送信し、ＩＣカード９がセキュア電文を受信する場合の模式図である。
（１）上位装置８とＩＣカード９が公開鍵を交換していない場合には、先の実施の形態２の（１）～（３）を行う。
（２）上位装置８は公開鍵１３を使用してＩＣカード９に送信する平文２１を暗号化し暗号文２２を作成する。
（３）上位装置８は暗号文２２よりハッシュ値２３を作成する。
（４）上位装置８はハッシュ値２３と秘密鍵１０よりメッセージ認証子２４を作成する。
（５）上位装置８はメッセージ認証子２４を添付した暗号文２２をＩＣカード９に対して送信する。
（６）メッセージ認証子２４を添付した暗号文２２を受信したＩＣカード９は暗号文２２からハッシュ値２５を作成する。
（７）ＩＣカード９はメッセージ認証子２４を公開鍵１１を用いて復号化する。
（８）ＩＣカード９は復号化したハッシュ値２６と作成したハッシュ値２５を比較する。
（９）ＩＣカード９は暗号文２２を秘密鍵１２を使用して復号化し、ＩＣカードより送信された平文２７を取りだす。
【００２２】
通信終了後はＩＣカード９内にある公開鍵１１、秘密鍵１２及び公開鍵１３を廃棄し、次回起動時には新しい鍵を上位装置とＩＣカード９で生成し交換することにより、より高い不正解読防止かつ書き換え防止機能となる。
【００２３】
【発明の効果】
以上、本発明によれば、公開鍵暗号方式の鍵を使用したセキュアメッセージングを行うことにより、隠蔽性、完全性の高い電文を送信するセキュアメッセージングの方法を用いるＩＣカードおよびＩＣカード暗号方法を提供できる。これによって、ＩＣカードと上位装置間の通信において、より不正解読、かつ不正書き換えが困難な通信が可能となる。
【図面の簡単な説明】
【図１】本発明の実施の形態１によるＩＣカードの構成図。
【図２】本発明の実施の形態２によるＩＣカードの暗号方法の模式図、ＩＣカードがセキュア電文を送信し、上位装置がセキュア電文を受信する場合の模式図。
【図３】本発明の実施の形態３によるＩＣカードの暗号方法の模式図、上位装置がセキュア電文を送信し、ＩＣカードがセキュア電文を受信する場合の模式図。
【符号の説明】

１，９　　ＩＣカード
２　　揮発性メモリ
３　　読み出し専用不揮発性メモリ
４　　読み出し書き込み可能専用不揮発性メモリ
５　　演算処理部
６　　インターフェース
７，８　　上位装置
１０，１２　　秘密鍵
１１，１３　　公開鍵
１４，２０，２１，２７　　平文
１５，２２　　暗号文
１６，１８，１９，２３，２５，２６　　ハッシュ値
１７，２４　　メッセージ認証子

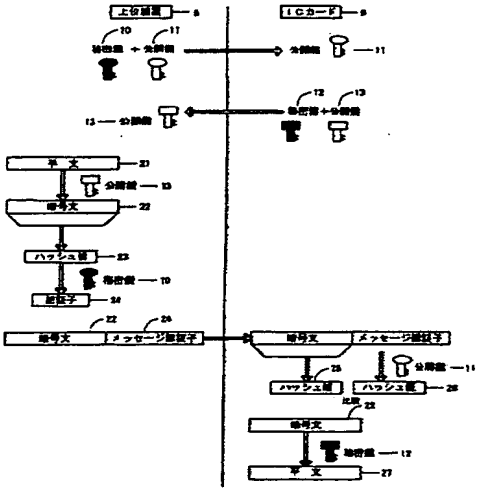
【図１】



【図２】



【図３】


ICカード
平文
暗号文
ハッシュ値
暗号文
メッセージ認証子
暗号文
メッセージ認証子
ハッシュ値
ハッシュ値
暗号文
平文

フロントページの続き

(51) Int.Cl.[7]		F I		
テーマコード（参考）				
Ｈ０４Ｌ	9/10	Ｈ０４Ｌ	9/00	６０１Ｆ
Ｈ０４Ｌ	9/32	Ｈ０４Ｌ	9/00	６７５Ｂ